- 2 -

IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method executed utilizing a computer including a
    tangible computer readable medium for prioritized network security, comprising:

(a)   identifying a set of policies, each policy having a condition associated therewith;

(b)   determining whether the conditions are met; and

(c)   activating the policies whose associated conditions are determined to be met;

(d)   wherein the conditions represent a priority of the policy;

(e)   wherein a first policy with a higher priority has a first condition associated
       therewith that is different from a second condition associated with a second policy
       with a lower priority such that the first policy and second policy are activated
       under different priority-related conditions;

(f)   wherein the activation of the policies includes:

            adding the policies to a set of a plurality of active policies, and executing
       security actions associated with the active policies if associated limits are met;
       and

            identifying currently executed security actions, determining whether a
       conflict exists between the currently executed security actions, and resolving any
       conflicts between the currently executed security actions;

(g)   wherein the conditions include a time factor, the time factor including at least one
       of a timeframe, a predetermined time period, and a time limit;

(h)   wherein the conditions include a source of the policies.

2. (Original) The method as recited in claim 1, and further comprising determining
    whether a user confirms the activation of the policies.

3. (Original) The method as recited in claim 2, and further comprising activating the
    policies if the user confirms.

- 3 -

4. (Original) The method as recited in claim 1, and further comprising updating the set of policies.

5. (Original) The method as recited in claim 4, wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy.

6. (Cancelled)

7. (Previously Presented) The method as recited in claim 1, and further comprising determining whether the conditions associated with the active policies are still met, and de-activating the active policies if the associated conditions are not met.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Original) The method as recited in claim 1, wherein the conditions include a severity of security actions associated with the policies.

12. (Currently Amended) A computer program product embodied on a tangible computer readable medium for prioritized network security, comprising:

(a) computer code for identifying a set of policies, each policy having a condition associated therewith;

(b) computer code for determining whether the conditions are met; and

(c) computer code for activating the policies whose associated conditions are determined to be met;

(d) wherein the conditions represent a priority of the policy;

- 4 -

(e)   wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions;

(f)   wherein the activation of the policies involves:

computer code for adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

computer code for identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;

(g)   wherein the conditions include a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

(h)   wherein the conditions include a source of the policies.

13.   (Original) The computer program product as recited in claim 12, and further comprising computer code for determining whether a user confirms the activation of the policies.

14.   (Original) The computer program product as recited in claim 13, and further comprising computer code for activating the policies if the user confirms.

15.   (Original) The computer program product as recited in claim 12, and further comprising computer code for updating the set of policies.

16.   (Original) The computer program product as recited in claim 15, wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy.

-5-

17. (Cancelled)

18. (Previously Presented) The computer program product as recited in claim 12, and further comprising computer code for determining whether the conditions associated with the active policies are still met, and de-activating the active policies if the associated conditions are not met.

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Original) The computer program product as recited in claim 12, wherein the conditions include a severity of security actions associated with the policies.

23. (Currently Amended) A system including a computer with a tangible computer readable medium for prioritized network security, comprising:

(a) logic for identifying a set of policies, each policy having a condition associated therewith;

(b) logic for determining whether the conditions are met; and

(c) logic for activating the policies whose associated conditions are determined to be met;

(d) wherein the conditions represent a priority of the policy;

(e) wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions;

(f) wherein the activation of the policies involves:

- 6 -

logic for adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

logic for identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;

(g)   wherein the conditions include a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

(h)   wherein the conditions include a source of the policies.

24.   (Cancelled)

25.   (Cancelled)

26.   (Cancelled)

27.   (Cancelled)

28.   (Currently Amended) A method executed utilizing a computer including a tangible computer readable medium for prioritized network security, comprising:

(a)   identifying a set of policies, each policy having a condition associated therewith;

(b)   determining whether the conditions are met; and

(c)   activating the policies whose associated conditions are determined to be met;

(d)   wherein the conditions represent an urgency associated with an issue causing the policy to be activated;

(e)   wherein a first policy with a higher associated urgency has a first condition associated therewith that is different from a second condition associated with a second policy with a lower associated urgency such that the first policy and the second policy are activated under different urgency-related conditions;

(f)   wherein the activation of the policies includes:

- 7 -

adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions

(g)   wherein the conditions include a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

(h)   wherein the conditions include a source of the policies.

29.   (Currently Amended) A method executed utilizing a computer including a tangible computer readable medium for providing network security, comprising:

(a)   identifying a set of a plurality of inactive policies each including a security action, a condition for activating the policy, and a limit for triggering the security action if the policy is active;

(b)   updating the set of inactive policies including:

    (i)   receiving another inactive policy,

    (ii)   determining whether the user accepts the inactive policy, and

    (iii)   adding the inactive policy to the set if the user accepts the inactive policy;

(c)   determining whether the conditions are met for the inactive policies;

(d)   determining whether a user confirms the activation of the inactive policies if the associated conditions are met; and

(e)   activating the inactive policies if the user confirms, the activation including:

    (i)   adding the inactive policies to a set of a plurality of active policies,

    (ii)   determining whether the conditions associated with the active policies are still met,

    (iii)   de-activating the active policies if the associated conditions are not met, and

    (iv)   executing the security actions associated with the active policies if the associated conditions are met and the limits are met, the execution of the security actions including:

- 8 -

    (1)   identifying currently executed security actions,

    (2)   determining whether a conflict exists between the currently executed security actions, and

    (3)   resolving any conflicts between the currently executed security actions;

(f)   wherein the conditions include a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

(g)   wherein the conditions include a source of the policies.

30.   (Previously Presented) The method as recited in claim 1, wherein the policies include low priority policies that are default policies which do not expire.

31.   (Previously Presented) The method as recited in claim 1, wherein the policies include medium priority policies that are valid for the predetermined time period.

32.   (Previously Presented) The method as recited in claim 31, wherein the policies include high priority policies that are valid for another predetermined time period that is less than the predetermined time period associated with the medium priority policies.

33.   (Previously Presented) The method as recited in claim 1, wherein the identifying the set of policies, the determining whether the conditions are met, and the activating the policies are controlled locally.